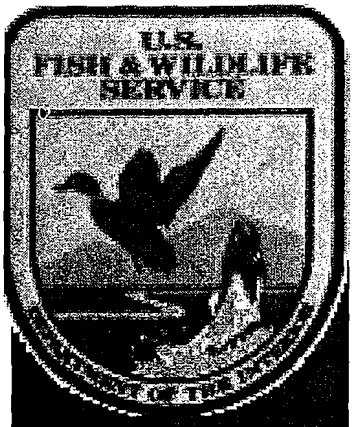

U.S. Department of the Interior
U.S. Fish and Wildlife Service

Information Technology Security Requirements for Acquisition – Guide

Version 1.0

04/11/2005

Information Resources and Technology Management (IRTM)
Region 9 - Washington Office

Table of Contents

1 OVERVIEW **3**

2 REQUIREMENTS FOR ACQUISITIONS AND CONTRACTUAL AGREEMENTS **3**

3 PROCESSES **3**

3.1 GUIDELINES TO PROGRAM MANAGER OR IT SYSTEM OWNER TASKS 4
3.2 GUIDELINES TO CONTRACTING OFFICER TASKS 5
3.3 GUIDELINES TO INFORMATION SECURITY PERSONNEL TASKS 5

4 DOI AND USFWS CROSS REFERENCED REQUIREMENTS **6**

4.1 COMMERCIAL OFF-THE-SHELF (COTS) HARDWARE OR SOFTWARE 6
4.2 DEVELOPMENT OR MAINTENANCE OF CUSTOM APPLICATIONS SERVICES 6
4.3 OUTSOURCED IT SERVICES OR ON-SITE SUPPORT SERVICES 13

APPENDIX A: INFORMATION SECURITY CONTACT LIST **19**

APPENDIX B: REFERENCES **20**

FEDERAL REFERENCES 20
FEDERAL INFORMATION PROCESSING STANDARDS 21
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) REFERENCES 21
DEPARTMENT OF THE INTERIOR (DOI) REFERENCES 23
U.S. FISH AND WILDLIFE REFERENCES 24

1 Overview

In accordance with the requirements of the Departmental Manual (DM) 375, Chapter 19, every Department of Interior (DOI) procurement solicitation documentation such as Request for Proposals (RFP), Requests For Information (RFI), Statements of Work (SOW), Statements of Requirements (SOR), etc. that involve the development of an Information Technology (IT) system or the use of DOI information resources, must include appropriate Information Security requirements. Information Security requirements must be considered in all phases of the DOI procurement cycle: planning, solicitation, source selection/award, and contract administration.

This DOI Office of the Chief Information Officer (OCIO) DOI OCIO Memorandum titled, *Information Security Requirements for Acquisition*, dated August 18, 2004, describes the Information Security policy for establishing Information Security requirements for DOI IT–related procurements. All DOI contract-awarding officials must adhere to the policy guidelines presented in this bulletin, whether the IT-related services are procured by DOI or other Federal government organizations on behalf of DOI.

2 Requirements for Acquisitions and Contractual Agreements

All contractors and other external organizations who are involved in developing information systems for use by DOI, or in providing any other type of service for DOI in which Federal information resources are used, must comply with the guidance in the DOI OCIO Memo referenced above.

Information Security requirements will be considered in all phases or stages of the DOI procurement process. The applicable Program Manager/information system Owner is responsible for ensuring that the solicitation document includes the appropriate Information Security requirements. The Information Security requirements must be sufficiently detailed to enable service providers to understand what is required. A general statement that the service provider must agree to comply with applicable requirements is not acceptable. At a minimum DOI requires that the Information Security requirements in the solicitation documents address the minimum DOI information system security requirements contained in Appendix C, DOI IT System Security Requirements. The applicable DOI Program Manager/information system is responsible for ensuring that the minimum DOI information system security requirements are implemented and complied with for any information system under their management control or purview. The applicable DOI Program Manager/information system will involve the appropriate Information Security personnel from the beginning of the procurement lifecycle for any IT-related procurement.

3 Processes

The recommended general processes for implementing Information Security requirements in IT-related contracts are as follows:

3.1 Guidelines to Program Manager or IT System Owner Tasks

1. Identify Information Security and privacy requirements during the requirements analysis based on a specific analysis of availability, integrity, and confidentiality and the technical requirements of the contract.

2. Use Federal Information Processing Standard (FIPS) 199 and the DOI Asset Valuation Guide to determine system sensitivity and criticality.

3. Ensure that all hardware and software purchases conform to the current version of the DOI Technical Reference Model (TRM) (see www.doi.gov/ocio/architecture).

4. Ensure that all system development efforts comply with the best practices, technical standards and product standards identified in the current version of the DOI Technical Reference Model (see www.doi.gov/ocio/architecture).

5. Determine which Information Security measures will be necessary to protect Sensitive but Unclassified (SBU) information by listing the potential threats and vulnerabilities and then describing the measures needed to provide protection, including physical and environmental security safeguards. See 375 DM 19 for more detail concerning SBU information.

6. If information sharing is involved, resolve any conflicts among all affected information owners or custodians and establish whatever MOUs or MOAs are necessary. In general, the information owner or custodian will establish the security level for their respective information.

7. Develop specifications (either a Statement of Work or Performance Work Statement) that include appropriate Information Security requirements and address appropriate technical, administrative, physical and personnel security requirements.

8. Develop evaluation criteria for use in the selection of the contractor.

9. Participate in evaluation of the proposals received in response to the DOI procurement document to ensure that they address and meet the minimum Information Security requirements and make a source selection recommendation.

10. Undergo appropriate training to qualify as a Contracting Officer's Representative (COR) and serve as a COR as necessary.

11. Prior to implementing any software configuration changes, obtain approval of the applicable Configuration/Change Control Board or Architectural Review Board. If no board exists, consult with the OCIO, Chief Technical Officer on the proper course of action.

12. Prior to being moved into production, obtain approval of the applicable Technical Review Board, Configuration/Change Control Board or Architectural Review Board

(ARB) for all software updates. Ensure the Independent Verification and Validation (IV&V) is performed. If no board exists, consult with the OCIO, Chief Technical Officer (CTO) on the proper course of action.

13. Ensure that periodic reviews of the project are conducted to ascertain whether Information Security has been maintained at the appropriate level and compliance with the Information Security Program continued after award. All instances of noncompliance should be reported to the Contracting Officer or designated representative, for necessary action.

14. Conduct closeout activities, including return of all SBU information and information resources provided during the life of this contract at the expiration or completion of this contract.

3.2 Guidelines to Contracting Officer Tasks

1. Support the Program Manager or Information System Owner during the requirements analysis phase by conducting market research and providing procurement planning assistance as needed.

2. Review incoming Statements of Work (SOWs) and Performance Work Statements for IT-related acquisitions to ensure that Information Security has been addressed. If it has not, coordinate with the requisitioner to ensue compliance with the DOI Information Security program.

3. Include Information Security as an evaluation factor in IT-related acquisitions and ensure that Information Security interests are represented during the evaluation period.

4. Appoint Contracting Officer's Technical Representatives (COTRs) who are knowledgeable in Information Security. If appropriate, appoint special COTRs with authority limited to Information Security matters in addition to general COTRs.

3.3 Guidelines to Information Security Personnel Tasks

1. Support the Program Manager or Information System Owner during the requirements analysis phase by evaluating requirements and providing advice on appropriate security measures.

2. Review proposed Statements of Work and Performance Work Statements to ensure that the resulting contracts sufficiently define Information Security responsibilities, provide a means to respond to Information Security problems, and include a right to terminate the contract if it can be shown that the contractor does not abide by the Information Security terms of the contract.

3. Participate in evaluation of offers to ensure that Information Security requirements are adequately addressed.

4. Approve contractors' IT security Certification and Accreditation (C&A) documents in a timely manner.

5. Undergo appropriate training to qualify as COTRs and serve as COTRs as necessary.

4 DOI and USFWS Cross Referenced Requirements

The security requirements addressed below are required in all RFPs, RFIs, SOWs, SORs, etc. that involve the development of an information system or the use of DOI information resources, must include appropriate Information Security requirements.

The following sections describe the Departmental requirement and how the Service will implement the requirement.

4.1 Commercial Off-the-Shelf (COTS) Hardware or Software

If you are buying **Commercial Off-the-Shelf (COTS) Hardware or Software**, you must put the following requirement(s) in the SOW or constraint in the Performance Work Statement:

DOI Requirement	Service Implementation
Quality Control All software and hardware must be free of malicious code.	All software/hardware purchased must be free of malicious code such as viruses, Trojan horse programs, worms, spyware, etc. Validation of this must be written into the contract. Malicious code or malware (short for malicious software) is defined as software (or firmware) designed to damage or do other unwanted actions on a computer system. Common examples of malware include viruses, worms, Trojan horses and spyware. Viruses, for example, can cause havoc on a computer's hard drive by deleting files or directory information. Spyware can gather data from a user's system without the user knowing it. This can include anything from the web pages a user visits to personal information, such as credit card numbers.

4.2 Development or Maintenance of Custom Applications Services

If you are buying **Development or Maintenance of Custom Applications Services**, you must put the following requirement(s) in the SOW or constraint in the Performance Work Statement:

DOI Requirement	Service Implementation
Background Investigations Contractor employees who will have access to DOI information or will develop custom applications are subject to background investigations. The level/complexity of background investigations must be the same as for a Federal employee holding a similar position; DM441, Chapter 3, provides guidance for the	**Background Investigations** Contractors and contractor employees acting for or on behalf of the Department of the Interior must obtain, and maintain, a favorably adjudicated background investigation at a level equal to that which would be conducted for a federal employee with similar duties and responsibilities. Contact the Division of Human

appropriate background investigations based on types of access. The solicitation and contract should state the levels required for applicable labor categories or positions. Ordinarily, the vendor should be responsible for paying the cost the background investigations. Existing clearances at the same or higher levels may be accepted. The request forms should be included in the solicitation if possible. Work cannot begin on the DOI system until the background investigation has at least been initiated.	Resources for specific information concerning background checks (i.e. investigation types based on job role, associated costs).
Non-disclosure Agreement Contractor employees who will have access to DOI or Service information or will develop custom applications must sign a non-disclosure agreement prior to gaining access. Each agreement must be tailored to the contract; however, a sample agreement follows this matrix. A draft or sample agreement may be included in solicitations. After award, the COR will develop the final agreements, with the assistance of the Solicitor.	**Non-disclosure Agreement** All contract employees who will have access to DOI/Service information (this includes information systems) or will develop custom applications for use in DOI/USFWS must sign and submit a non-disclosure agreement. Copies the completed non-disclosure agreement(s) will be maintained in the contract file. The standard USFWS Non-Disclosure Form can be found at http://forms.fws.gov/3-2235.pdf.
Training Contractor employees must take DOI's end-user computer security awareness training prior to being granted access to DOI data or being issued a user account. Training must be renewed annually.	**Training** All contract employees must take the DOI IT Security Awareness Training, this is an annual requirement for all DOI and Service employees (government and contract). Additionally, the contract employees must sign a Statement of Responsibility (SOR) that states they have read the USFWS IT Appropriate Use Policy and other applicable IT security policies. The FY 2005 DOI Information Security Awareness Training can be found at http://www.doiu.nbc.gov/itsecurity/ or be provided by the RITSMs on CD-ROM. The USFWS Statement of Responsibility (SOR) can be found at http://forms.fws.gov/3-2212.pdf. The training and copies of IT security policy can be obtained from the Regional Information Technology Security Managers (RITSMs).
Contractor Location Custom software development and outsourced operations must be located in the United States to the maximum extent practical. If such services are proposed to be performed abroad, the contractor must provide an acceptable security plan specifically to address mitigation of the resulting problems of communication, control, data protection, and so forth. Location within the U.S. may be an evaluation factor.	**Contractor Location** If custom software is going to be developed and outsourced for use by DOI or the Service, it must be developed and outsourced in the United States, as is practicable. If these services are to be performed outside of the United States, the contractor must provide a security plan that addresses the mitigation of problems such as communication, operational control of development, how the data will be protected (i.e. encryption, physical security), etc. It is incumbent upon the customer to research and verify this requirement. This requirement must be written into the contract.
Applicable Standards Contractors must follow the DOI System Development Life Cycle (SDLC), NIST SP 800-64 and the DOI	**Applicable Standards** Solicitations must include either the complete publications or a reference to public facilities, such as a

SDLC Security Integration Guide. Solicitations must include either the complete publications or a reference to public facilities, such as a website or office, where they may be accessed.	website or office, where they may be accessed. Copies of these documents can be obtained by contacting your RITSM. See Appendix B of this document. Contact the Branch of Data and Systems Services (BDSS) in the Division of Information Resources and Technology Management (IRTM) for detailed information concerning the DOI SDLC or the USFWS SDLC. The BDSS has a variety of responsibilities that can be divided into two primary functions: Data Administration and Systems Development. The branch is also responsible for maintaining the Service Information and Technology Architecture (SITA).
Asset Valuation The Contractor must use the DOI Asset Valuation Guide for all systems to determine mission impact, data sensitivity, risk level, bureau/departmental/national criticality, and whether the system is a Major Application, Minor Application, or General Support System. Solicitations must include either the complete publication or a reference to public facilities, such as a website or office, where it may be accessed.	**Asset Valuation** The DOI Asset Valuation Guide provides a structured method for classifying a system as a general support system (GSS), major application (MA), contractor operated or minor application. This guide will assist in consistently, properly and rapidly identifying the system classification for DOI information and information systems in compliance with Federal mandates. Each Federal agency is required to provide a cost-effective set of security controls to protect their information and information systems from unauthorized disclosure. The required security controls are based upon many things including the system classification and data types processed which will be determined upon completion of the DOI Information Technology Security Needs Assessment Form (ITSNA) Survey Form in Appendix D of the Asset Valuation Guide. Contact your RITSM for questions concerning the Asset Valuation.
Property Rights DOI will own the intellectual property rights to any software developed on its behalf to the maximum extent practical. Generally, FAR 52.227-14, *Rights in Data-General*, and its alternates will be used in the contract. However, deviation from this policy may be necessary as circumstances warrant.	**Property Rights** The intellectual rights of any software developed for DOI/USFWS will be owned by DOI/USFWS. There may be exceptions to this – check the requirements in FAR 52.227-14 for more detail.
Independent Validation and Verification (IV&V) Software updates must be independently verified and validated prior to being moved into production. The solicitation and contract should be clear as to which party performs this function and is responsible for associated costs.	**Independent Validation and Verification (IV&V)** All updates to software must be tested and validated/verified by an independent third party. The contract must state specifically whether the Service or the contractor is responsible for this. Contact the RITSM for detailed information concerning IV&Vs.

Certification and Accreditation (C&A) Major Applications and General Support Systems must be certified and accredited (C&A) prior to going into production and reaccredited every three years or whenever there is a major change that affects security. C&A documents will be provided to the COR in both hard copy and electronic (specify) forms. The contractor must follow NIST SP 800-37, 800-18, 800-30, 800-60 vol. 1 and vol. 2, 800-53 - Annex 1, Annex 2 and Annex 3, Federal Information Processing Standard (FIPS) 199 and FIPS 200, the associated DOI guides/templates, the DOI Security Test & Evaluation (ST&E) Guide, and the DOI Privacy Impact Assessment. Solicitations must include either the complete publications or a reference to public facilities, such as a website or office, where they be accessed.	**Certification and Accreditation (C&A)** Any system categorized as a Major Application (MA) or General Support System (GSS) must undergo certification and accreditation activities before the system is placed in a production environment. Certification and Accreditation (C&A) is the formal test (certification) and acceptance (accreditation) of system security controls for information systems. It is a process that recognizes, evaluates, and assigns assumptive responsibility for the risk of operating an information system. The risk assessment of the system identifies threats, risks, and vulnerabilities of a system to damage and compromise. In the C&A process, the Service Designated Accrediting Authority (DAA) evaluates tests of security controls performed by the system certifier and determine whether the residual risk to the system (that risk which was not eliminated by implementation of countermeasures) is acceptable and that the functioning security controls provides adequate protection for the system to operate. The Service requires that Service personnel follow the C&A methodology in the Department of the Interior Certification and Accreditation Guide. Within the Service, application of this process is mandatory for C&A of information systems. System Owners must ensure every GSS and MA has been certified and are accredited. All information systems require certification as a prerequisite to accreditation. The Service uses the C&A methodology in the DOI C&A Guide.
The Government will reserve the right to conduct the Security Test and Evaluation (ST&E), using either Government personnel or an independent contractor.	The ST&E is a mandatory technical test that verifies that the security controls outlined in the C&A documentation are valid and meet the minimum DOI/USFWS standards. Generally, the system developer conducts the ST&E, but the Service reserves the right to conduct the ST&E or outsource it to an independent third party.
The contractor will take appropriate and timely action (this can be specified in the contract) to correct or mitigate any weaknesses discovered during such testing, generally at no additional cost.	If any security weaknesses are discovered as a result of the ST&E, the contractor must develop a plan to mitigate those weaknesses in a timely manner. The mitigation of these weaknesses should not result in additional costs to the Service.
The Designated Approving Authority (DAA) for the system will be the official identified in DOI Secretarial Order No. 3255.	Currently, the USFWS Director is the DAA. Contact your RITSM to for questions concerning the C&A process.
Incident Reporting The contractor must report computer security incidents affecting DOI data or systems in accordance with the	**Incident Reporting** Contractors must report any computer security incidents or suspected security incidents that affect Service data

DOI Computer Incident Response Guide. Solicitations must include either the complete publication or a reference to public facilities, such as a website or office, where it may be accessed.	or information systems in accordance with the Service Computer Security Incident Response Team Handbook. The USFWS guide mirrors requirements in the DOI guide. Contact your RITSM for questions concerning the Computer Security Incident Response process.
Quality Control All software and hardware must be free of malicious code.	**Quality Control** All software/hardware purchased must be free of malicious code such as viruses, Trojan horse programs, worms, spyware, etc. Validation of this must be written into the contract. Malicious code or malware (short for malicious software) is defined as software (or firmware) designed to damage or do other unwanted actions on a computer system. Common examples of malware include viruses, worms, Trojan horses and spyware. Viruses, for example, can cause havoc on a computer's hard drive by deleting files or directory information. Spyware can gather data from a user's system without the user knowing it. This can include anything from the web pages a user visits to personal information, such as credit card numbers.
Vulnerability Analysis All systems must be scanned monthly with a vulnerability analysis tool that is compatible with the software in use by the OCIO at the time (specify this in the solicitation). All "safe" or "non-destructive" checks must be turned on. All electronic copy of each report and session data will be provided to the COR. At least annually, all high risk systems and systems accessible from the Internet must be independently penetration tested. Electronic and hard copy reports of penetration test results will be provided to the COR.	**Vulnerability Analysis** All Service information systems must be scanned for vulnerabilities. All Service information systems are scanned with various vulnerability tools. Currently, the primary tool in use in the Service is called VAM (Vulnerability Assessment Monitor). Information systems maintained or residing at contractor sites must use VAM (or a compatible tool) and send an electronic report (at least monthly) to the COR who will forward the report to the RITSM. Details regarding VAM can be obtained from the RITSM. All Service high risk information systems (i.e. systems that contain financial, privacy, FOIA, Trust data) that are accessible from the Internet must have penetration tests conducted on them at least annually. A penetration test is a method of evaluating the security of a computer system or network by simulating an attack by a malicious hacker. The process involves an active analysis of the system for any weaknesses, technical flaws or vulnerabilities. This analysis is usually carried out from the position of a potential attacker, and can involve active exploitation of security vulnerabilities. Any security issues that are found will be presented to the system owner together with an assessment of their impact and often with a proposal for mitigation or a technical solution. The penetration test can be conducted by either an independent-third party or the Government, but the decision lies with the customer.

	Both, electronic and hard copy reports of penetration test results must be provided to the COR who will forward these to the RITSM.
The Government will reserve the right to conduct unannounced and prearranged independent vulnerability scans using Government personnel or another contractor.	The Service retains the right to conduct unannounced and/or prearranged vulnerability scans using Government personnel or independent third party. This requirement primarily concerns information systems maintained by the contractor or residing at contractor sites.
The contractor will take appropriate and timely action (this can be specified in the contract) to correct or mitigate any weaknesses discovered during such testing, generally at no additional cost.	If any security weaknesses are discovered as a result of the vulnerability scans, the contractor must develop a plan to mitigate those weaknesses in a timely manner. The mitigation of these weaknesses should not result in additional costs to the Service.
Logon Banner Contractor employees who will access DOI data must acknowledge a Government-approved logon warning prior to each logon to the system.	**Logon Banner** Contractor employees who access Service information systems must acknowledge a Government-approved Legal Warning Banner prior to them logging on to the system. This includes contractor owned information systems hosting Service data. The network warning banner communicates that there is no expectation of privacy in the authorized or unauthorized use of Service information systems. The use of warning banners on Service computers and networks provides legal notice to anyone accessing them that they are using a U.S. Government system that is subject to monitoring. Users should also be notified of the possible sanctions, such as loss of privileges or even prosecution, if they misuse or access the network without authorization. All Service systems must display warning banners upon connection to a given system. These banners will display a warning that states the system is for legitimate use only, is subject to monitoring, and carries no expectation of privacy. Service networks and information systems do not inherently provide users a right of privacy. As such, the Service reserves the right to monitor use in accordance with Department and USFWS Information Security Program policies. However, System Owners must notify users of monitoring prior to system access to avoid any question about an implied right to privacy on the system. The information contained in the banners is standard and must be approved by DOI's legal staff. All Service computers, workstations, laptops and other information resources will display a standard, DOI approved legal banner. Current wording for the banner can be obtained from your RITSM.

Security Controls Contractors will be required to ensure compliance with the security control requirements of the current version of NIST SP 800-53, Annex 1, Annex 2 and Annex 3 or Federal Information Processing Standard (FIPS) 200 (scheduled to be published in the Fall of 2005) that are appropriate to the sensitivity and criticality of the data or system. FIPS 199 and the DOI Asset Valuation Guide will be used to determine sensitivity and criticality. Solicitations must include either the complete publication or a reference to public facilities, such as a website or office, where they be accessed.	**Security Controls** Contractors must comply with the security controls in NIST SP 800-53 or FIPS 200 that are appropriate to the sensitivity and criticality of the data or system. For details concerning required security controls, contact your RITSM.

4.3 Outsourced IT Services or On-Site Support Services

If you are buying Outsourced IT Services or On-site Support services, you must put the following requirement(s) in the Statement of Work (SOW) or constraint in the Performance Work Statement:

DOI Requirement	Service Implementation
Background Investigations Contractor employees who will have access to DOI information or will develop custom applications are subject to background investigations. The level/complexity of background investigations must be the same as for a Federal employee holding a similar position; DM441, Chapter 3, provides guidance for the appropriate background investigations based on types of access. The solicitation and contract should state the levels required for applicable labor categories or positions. Ordinarily, the vendor should be responsible for paying the cost the background investigations. Existing clearances at the same or higher levels may be accepted. The request forms should be included in the solicitation if possible. Work cannot begin on the DOI system until the background investigation has at least been initiated.	**Background Investigations** Contractors and contractor employees acting for or on behalf of the Department of the Interior must obtain, and maintain, a favorably adjudicated background investigation at a level equal to that which would be conducted for a federal employee with similar duties and responsibilities. Contact the Division of Human Resources for specific information concerning background checks (i.e. investigation types based on job role, associated costs).
Non-disclosure Agreement Contractor employees who will have access to DOI or Service information or will develop custom applications must sign a non-disclosure agreement prior to gaining access. Each agreement must be tailored to the contract; however, a sample agreement follows this matrix. A draft or sample agreement may be included in solicitations. After award, the COR will develop the final agreements, with the assistance of the Solicitor.	**Non-disclosure Agreement** All contract employees who will have access to DOI/Service information (this includes information systems) or will develop custom applications for use in DOI/USFWS must sign and submit a non-disclosure agreement. Copies the completed non-disclosure agreement(s) will be maintained in the contract file. The standard USFWS Non-Disclosure Form can be found at http://forms.fws.gov/3-2235.pdf.
Training Contractor employees must take DOI's end-user computer security awareness training prior to being granted access to DOI data or being issued a user account. Training must be renewed annually.	**Training** All contract employees must take the DOI IT Security Awareness Training, this is an annual requirement for all DOI and Service employees (government and contract). Additionally, the contract employees must sign a Statement of Responsibility (SOR) that states they have read the USFWS IT Appropriate Use Policy and other applicable IT security policies. The FY 2005 DOI Information Security Awareness Training can be found at http://www.doiu.nbc.gov/itsecurity/ or be provided by the RITSMs on CD-ROM. The USFWS Statement of Responsibility (SOR) can be found at http://forms.fws.gov/3-2212.pdf. The training and copies of IT security policy can be obtained from the Regional Information Technology Security Managers (RITSMs).

Personnel Changes The contractor must notify the COR immediately when an employee working on a DOI system is reassigned or leaves the contractor's employ, and prior to an unfriendly termination.	**Personnel Changes** Anytime a contract employee leaves the contract or is reassigned, the COR must be contacted immediately by the contract company. For unfriendly terminations, the COR must be contacted PRIOR to the termination, as is practicable.
Contractor Location Custom software development and outsourced operations must be located in the United States to the maximum extent practical. If such services are proposed to be performed abroad, the contractor must provide an acceptable security plan specifically to address mitigation of the resulting problems of communication, control, data protection, and so forth. Location within the U.S. may be an evaluation factor.	**Contractor Location** If custom software is going to be developed and outsourced for use by DOI or the Service, it must be developed and outsourced in the United States, as is practicable. If these services are to be performed outside of the United States, the contractor must provide a security plan that addresses the mitigation of problems such as communication, operational control of development, how the data will be protected (i.e. encryption, physical security), etc. It is incumbent upon the customer to research and verify this requirement. This requirement must be written into the contract.
Asset Valuation The Contractor must use the DOI Asset Valuation Guide for all systems to determine mission impact, data sensitivity, risk level, bureau/departmental/national criticality, and whether the system is a Major Application, Minor Application, or General Support System. Solicitations must include either the complete publication or a reference to public facilities, such as a website or office, where it may be accessed.	**Asset Valuation** The DOI Asset Valuation Guide provides a structured method for classifying a system as a general support system (GSS), major application (MA), contractor operated or minor application. This guide will assist in consistently, properly and rapidly identifying the system classification for DOI information and information systems in compliance with Federal mandates. Each Federal agency is required to provide a cost-effective set of security controls to protect their information and information systems from unauthorized disclosure. The required security controls are based upon many things including the system classification and data types processed which will be determined upon completion of the DOI Information Technology Security Needs Assessment Form (ITSNA) Survey Form in Appendix D of the Asset Valuation Guide. Contact your RITSM for questions concerning the Asset Valuation.
Property Rights DOI will own the intellectual property rights to any software developed on its behalf to the maximum extent practical. Generally, FAR 52.227-14, *Rights in Data-General*, and its alternates will be used in the contract. However, deviation from this policy may be necessary as circumstances warrant.	**Property Rights** The intellectual rights of any software developed for DOI/USFWS will be owned by DOI/USFWS. There may be exceptions to this – check the requirements in FAR 52.227-14 for more detail.
Independent Validation and Verification (IV&V) Software updates must be independently verified and validated prior to being moved into production. The solicitation and contract should be clear as to which party performs this function and is responsible for associated costs.	**Independent Validation and Verification (IV&V)** All updates to software must be tested and validated/verified by an independent third party. The contract must state specifically whether the Service or the contractor is responsible for this. Contact the RITSM for detailed information concerning IV&Vs.
Certification and Accreditation (C&A)	

Major Applications and General Support Systems must be certified and accredited (C&A) prior to going into production and reaccredited every three years or whenever there is a major change that affects security. C&A documents will be provided to the COR in both hard copy and electronic (specify) forms. The contractor must follow NIST SP 800-37, 800-18, 800-30, 800-60 vol. 1 and vol. 2, 800-53 - Annex 1, Annex 2 and Annex 3, Federal Information Processing Standard (FIPS) 199 and FIPS 200, the associated DOI guides/templates, the DOI Security Test & Evaluation (ST&E) Guide, and the DOI Privacy Impact Assessment. Solicitations must include either the complete publications or a reference to public facilities, such as a website or office, where they be accessed.	Any system categorized as a Major Application (MA) or General Support System (GSS) must undergo certification and accreditation activities before the system is placed in a production environment. Certification and Accreditation (C&A) is the formal test (certification) and acceptance (accreditation) of system security controls for information systems. It is a process that recognizes, evaluates, and assigns assumptive responsibility for the risk of operating an information system. The risk assessment of the system identifies threats, risks, and vulnerabilities of a system to damage and compromise. In the C&A process, the Service Designated Accrediting Authority (DAA) evaluates tests of security controls performed by the system certifier and determine whether the residual risk to the system (that risk which was not eliminated by implementation of countermeasures) is acceptable and that the functioning security controls provides adequate protection for the system to operate. The Service requires that Service personnel follow the C&A methodology in the Department of the Interior Certification and Accreditation Guide. Within the Service, application of this process is mandatory for C&A of information systems. System Owners must ensure every GSS and MA has been certified and are accredited. All information systems require certification as a prerequisite to accreditation. The Service uses the C&A methodology in the DOI C&A Guide.
The Government will reserve the right to conduct the Security Test and Evaluation (ST&E), using either Government personnel or an independent contractor.	The ST&E is a mandatory technical test that verifies that the security controls outlined in the C&A documentation are valid and meet the minimum DOI/USFWS standards. Generally, the system developer conducts the ST&E, but the Service reserves the right to conduct the ST&E or outsource it to an independent third party.
The contractor will take appropriate and timely action (this can be specified in the contract) to correct or mitigate any weaknesses discovered during such testing, generally at no additional cost.	If any security weaknesses are discovered as a result of the ST&E, the contractor must develop a plan to mitigate those weaknesses in a timely manner. The mitigation of these weaknesses should not result in additional costs to the Service.
The Designated Approving Authority (DAA) for the system will be the official identified in DOI Secretarial Order No. 3255.	Currently, the USFWS Director is the DAA. Contact your RITSM to for questions concerning the C&A process.
Internet Logon Banner A Government-approved logon banner must be displayed on the first page of any public access web pages.	**Internet Logon Banner** A DOI-approved internet logon banner must be displayed on the first page of any publicly accessible web pages owned by DOI/USFWS.

	The information contained in the banner is standard and must be approved by DOI's legal staff. Current wording for the banner can be obtained from the RITSM.
Incident Reporting The contractor must report computer security incidents affecting DOI data or systems in accordance with the DOI Computer Incident Response Guide. Solicitations must include either the complete publication or a reference to public facilities, such as a website or office, where it may be accessed.	**Incident Reporting** Contractors must report any computer security incidents or suspected security incidents that affect Service data or information systems in accordance with the Service Computer Security Incident Response Team Handbook. The USFWS guide mirrors requirements in the DOI guide. Contact your RITSM for questions concerning the Computer Security Incident Response process.
Quality Control All software and hardware must be free of malicious code.	**Quality Control** All software/hardware purchased must be free of malicious code such as viruses, Trojan horse programs, worms, spyware, etc. Validation of this must be written into the contract. Malicious code or malware (short for malicious software) is defined as software (or firmware) designed to damage or do other unwanted actions on a computer system. Common examples of malware include viruses, worms, Trojan horses and spyware. Viruses, for example, can cause havoc on a computer's hard drive by deleting files or directory information. Spyware can gather data from a user's system without the user knowing it. This can include anything from the web pages a user visits to personal information, such as credit card numbers.
Self Assessment The contractor must conduct an annual self assessment in accordance with NIST SP 800-26 on all MAs, GSSs, and outsourced applications in production or a reference to public facilities, such as a website or office, where it may be accessed. Both hard copy and electronic copies of the assessment will be provided to the COR. The Government will reserve the right to conduct such an assessment using Government personnel or another contractor. The contractor will take appropriate and timely action (this can be specified in the contract) to correct or mitigate any weaknesses discovered during such testing, generally at no additional cost.	**Self Assessment** The Service requires self-assessments be conducted on all Service MAs, GSSs and outsourced applications. These self-assessments are based on guidance in NIST SP 800-26. Contact your RITSM to for questions concerning self-assessments.
Vulnerability Analysis All systems must be scanned monthly with a vulnerability analysis tool that is compatible with the software in use by the OCIO at the time (specify this in the solicitation). All "safe" or "non-destructive" checks must be turned on. All electronic copy of each report and session data will be provided to the COR.	**Vulnerability Analysis** All Service information systems must be scanned for vulnerabilities. All Service information systems are scanned with various vulnerability tools. Currently, the primary tool in use in the Service is called VAM (Vulnerability Assessment Monitor). Information systems maintained or residing at contractor sites must use VAM (or a compatible tool) and send an electronic report (at least monthly) to the COR who will forward the report to the RITSM. Details regarding VAM can

	be obtained from the RITSM.
At least annually, all high risk systems and systems accessible from the Internet must be independently penetration tested. Electronic and hard copy reports of penetration test results will be provided to the COR.	All Service high risk information systems (i.e. systems that contain financial, privacy, FOIA, Trust data) that are accessible from the Internet must have penetration tests conducted on them at least annually. A penetration test is a method of evaluating the security of a computer system or network by simulating an attack by a malicious hacker. The process involves an active analysis of the system for any weaknesses, technical flaws or vulnerabilities. This analysis is usually carried out from the position of a potential attacker, and can involve active exploitation of security vulnerabilities. Any security issues that are found will be presented to the system owner together with an assessment of their impact and often with a proposal for mitigation or a technical solution. The penetration test can be conducted by either an independent-third party or the Government, but the decision lies with the customer. Both, electronic and hard copy reports of penetration test results must be provided to the COR who will forward these to the RITSM.
The Government will reserve the right to conduct unannounced and prearranged independent vulnerability scans using Government personnel or another contractor.	The Service retains the right to conduct unannounced and/or prearranged vulnerability scans using Government personnel or independent third party. This requirement primarily concerns information systems maintained by the contractor or residing at contractor sites.
The contractor will take appropriate and timely action (this can be specified in the contract) to correct or mitigate any weaknesses discovered during such testing, generally at no additional cost.	If any security weaknesses are discovered as a result of the vulnerability scans, the contractor must develop a plan to mitigate those weaknesses in a timely manner. The mitigation of these weaknesses should not result in additional costs to the Service.
Logon Banner Contractor employees who will access DOI data must acknowledge a Government-approved logon warning prior to each logon to the system.	**Logon Banner** Contractor employees who access Service information systems must acknowledge a Government-approved Legal Warning Banner prior to them logging on to the system. This includes contractor owned information systems hosting Service data. The network warning banner communicates that there is no expectation of privacy in the authorized or unauthorized use of Service information systems. The use of warning banners on Service computers and networks provides legal notice to anyone accessing them that they are using a U.S. Government system that is subject to monitoring. Users should also be notified of the possible sanctions, such as loss of privileges or even prosecution, if they misuse or access the network without authorization. All Service systems must display warning banners upon connection

	to a given system. These banners will display a warning that states the system is for legitimate use only, is subject to monitoring, and carries no expectation of privacy. Service networks and information systems do not inherently provide users a right of privacy. As such, the Service reserves the right to monitor use in accordance with Department and USFWS Information Security Program policies. However, System Owners must notify users of monitoring prior to system access to avoid any question about an implied right to privacy on the system. The information contained in the banners is standard and must be approved by DOI's legal staff. All Service computers, workstations, laptops and other information resources will display a standard, DOI approved legal banner. Current wording for the banner can be obtained from your RITSM.
Security Controls Contractors will be required to ensure compliance with the security control requirements of the current version of NIST SP 800-53, Annex 1, Annex 2 and Annex 3 or Federal Information Processing Standard (FIPS) 200 (scheduled to be published in the Fall of 2005) that are appropriate to the sensitivity and criticality of the data or system. FIPS 199 and the DOI Asset Valuation Guide will be used to determine sensitivity and criticality. Solicitations must include either the complete publication or a reference to public facilities, such as a website or office, where they be accessed.	**Security Controls** Contractors must comply with the security controls in NIST SP 800-53 or FIPS 200 that are appropriate to the sensitivity and criticality of the data or system. For details concerning required security controls, contact your RITSM.
Contingency Plan The contractor will submit a contingency plan in accordance with NIST SP 800-34 and the DOI Contingency Plan Guide. Solicitations must include either the complete publications or a reference to public facilities, such as a website or office, where they may be accessed. The plan must be approved by the COR. A copy of the annual test results will be provided to the COR.	**Contingency Plan** The contractor will submit a contingency plan in accordance with NIST SP 800-34 and the DOI Contingency Plan Guide. This requirement concerns Service systems residing at contractor controlled sites or on contractor-owned systems that host DOI/Service data. For details concerning contingency planning, contact your RITSM.

Appendix A: Information Security Contact List

Chief Information Security Officer (CISO)
Primary: David B Smith - (703) 358-1905
Alternate: Lan Nguyen - (703) 358-1819

National Network Security Manager (NNSM)
Primary: TBD
Alternate: Warren Jernigan - (303) 275-2433

Region 1 Regional Information Technology Security Manager (RITSM)
Primary: Tyler Marriott - (503) 231-6294
Alternate: Doug Robertson - (503) 231-2023

Region 2 Regional Information Technology Security Manager (RITSM)
Primary: Jim Dukes - (505) 248-6888
Alternate: Tim Wise - (505) 248-6888

Region 3 Regional Information Technology Security Manager (RITSM)
Primary: John Herron - (612) 713-5116
Alternate: Janice Whitney - (612) 713-5123

Region 4 Regional Information Technology Security Manager (RITSM)
Primary: Carolyn Hust - (404) 679-4129
Alternate: Phil Hart - (404) 679-4134

Region 5 Regional Information Technology Security Manager (RITSM)
Primary: Mary Conser - (413) 253-8331
Alternate: TBD

Region 6 Regional Information Technology Security Manager (RITSM)
Primary: Margaret Wolf - (303) 236-7894
Alternate: George Bowen - (303) 236-7917

Region 7 Regional Information Technology Security Manager (RITSM)
Primary: Mark Russell - (907) 786-3396
Alternate: Benjamin Sherburne - (907) 786-3405

Region 9 Regional Information Technology Security Manager (RITSM)
Primary: Lan Nguyen - (703) 358-1819
Alternate: TBD

Appendix B: References

Federal References

Privacy Act of 1974, P.L. 93-579, 5 U.S.C. 552a (1974)
http://www.usdoj.gov/foia/privstat.htm

Computer Security Act of 1987, P.L. 100-235 (1988)
http://csrc.nist.gov/ispab/csa_87.txt

Title III, Federal Information Security Management Act (FISMA) of 2002
http://thomas.loc.gov/cgi-bin/bdquery/z?d107:HR02458:|TOM:/bss/d107query.html|

Federal Manager's Financial Integrity Act (FMFIA) of 1982
http://www.whitehouse.gov/omb/financial/fmfia1982.html

Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*
http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html

Office of Management and Budget (OMB) Circular A-130, Appendix III, *Security of Federal Automated Information Resources*
http://www.whitehouse.gov/omb/circulars/a130/a130appendix_iii.html

Office of Management and Budget (OMB) Circular A-11, *Preparing and Submitting Budget Estimates*
http://www.whitehouse.gov/omb/circulars/a11/02toc.html

Office of Management and Budget (OMB) Circular A-123, *Management Accountability and Control*
http://www.whitehouse.gov/omb/circulars/a123/a123.html

Office of Management and Budget (OMB), Memorandum 00-07, *Incorporating and Funding Security in Information Systems Investments*
http://www.whitehouse.gov/omb/memoranda/m00-07.html

Office of Management and Budget (OMB) M-04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act (FISMA)*
http://www.whitehouse.gov/omb/memoranda/fy04/m04-25.pdf

Executive Order 10450 - *Security Requirements for Government Employment*
http://www.archives.gov/federal_register/codification/executive_order/10450.html

Executive Order 12674 - *Implementing Standards of Ethical Conduct for Employees of the Executive Branch*
http://www.usoge.gov/pages/laws_regs_fedreg_stats/lrfs_files/exeorders/eo12674.pdf

Code of Federal Regulations (CFR) Title 43 - *Public Lands: Interior* Part 2 - *Records and Testimony; Freedom of Information Act*
http://www.mrm.mms.gov/FOIA/cfr432A.htm

Code of Federal Regulations (CFR) Title 43 - *Public Lands: Interior* Part 2 - *Records and Testimony; Freedom of Information Act Regulations and Implementation of the Electronic Freedom of Information Act Amendments of 1996*
http://www.doi.gov/foia/FOIARegulations.pdf

Code of Federal Regulations (CFR) Title 5 Chapter XVI - *Office of Government Ethics* Part 2635 - *Standards of Ethical Conduct for Employees of the Executive Branch*
http://www.usoge.gov/pages/laws_regs_fedreg_stats/oge_regs/5cfr2635.html

Federal Information Processing Standards

FIPS 191, *Guideline for the Analysis of Local Area Network Security*
http://csrc.nist.gov/publications/fips/fips191/fips191.pdf

FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*
http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

FIPS 201, *Personal Identity Verification for Federal Employees and Contractors*
http://csrc.nist.gov/publications/fips/fips201/FIPS-201-022505.pdf

National Institute of Standards and Technology (NIST) References

NIST SP800-12, *An Introduction to Computer Security: The NIST Handbook*
http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf

NIST SP800-15, *Generally Accepted Principles and Practices for Securing Information Technology Systems*,
http://csrc.nist.gov/publications/nistpubs/800-15/SP800-15.PDF

NIST SP800-17, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*
http://csrc.nist.gov/publications/nistpubs/800-17/800-17.pdf

NIST SP800-18, *Guide for Developing Security Plans for Information Technology Systems*
http://csrc.nist.gov/publications/nistpubs/800-18/Planguide.Pdf

NIST SP800-26, *Security Self-Assessment Guide for IT Systems*
http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf

NIST SP800-30, *Risk Management Guide for Information Technology Systems*
http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

NIST SP800-34, *Contingency Planning Guide for IT Systems*
http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf

NIST SP800-35, *Guide to Selecting Information Security Services*
http://csrc.nist.gov/publications/nistpubs/800-35/NIST-SP800-35.pdf

NIST SP800-36, *Guide to Selecting Information Security Products*
http://csrc.nist.gov/publications/nistpubs/800-36/NIST-SP800-36.pdf

NIST SP800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*
http://csrc.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf

NIST SP800-42, *Guideline on Network Security Testing*
http://csrc.nist.gov/publications/nistpubs/800-42/NIST-SP800-42.pdf

NIST SP800-47, *Security Guide for Interconnecting IT Systems*
http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf

NIST SP800-47, *Security Guide for Interconnecting IT Systems*
http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf

NIST SP800-50, *Building an Information Security Awareness and Training Program*
http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

NIST SP800-53, *Recommended Security Controls for Federal Information Systems*
http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf

NIST SP800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories, Volumes 1 and 2*
http://csrc.nist.gov/publications/nistpubs/800-60/SP800-60V1-final.pdf
http://csrc.nist.gov/publications/nistpubs/800-60/SP800-60V2-final.pdf

NIST SP800-61, *Computer Security Incident Handling Guide*
http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf

NIST SP800-64, *Security Considerations in the Information System Development Lifecycle*
http://csrc.nist.gov/publications/nistpubs/800-64/NIST-SP800-64.pdf

NIST IR 5153 *Minimum Security Requirements for Multi-user Operating Systems* (March 1993).
http://csrc.nist.gov/publications/nistir/ir5153.txt

Department of the Interior (DOI) References

Departmental Manual Part 375, *IRM Program Management*

- Chapter 19: *Information Technology Security Program*
  http://elips.doi.gov/app_dm/act_getfiles.cfm?relnum=3397

Departmental Manual Part 441, *Personnel Suitability and Security Requirements*

- Chapter 1: *General Information*
  http://elips.doi.gov/app_dm/act_getfiles.cfm?relnum=3323

- Chapter 2: *Responsibilities*
  http://elips.doi.gov/app_dm/act_getfiles.cfm?relnum=3630

- Chapter 3: *Personnel Suitability and Security Requirements*
  http://elips.doi.gov/app_dm/act_getfiles.cfm?relnum=3631

- Chapter 5: *Adjudication Standards*
  http://elips.doi.gov/app_dm/act_getfiles.cfm?relnum=3290

Departmental Manual Part 444, *Physical Protection and Building Security*

- Chapter 1: *General Program Requirements*
  http://elips.doi.gov/app_dm/act_getfiles.cfm?relnum=3270

Department of the Interior (DOI), *Internet Acceptable Use Policy*
http://www.doiu.nbc.gov/orientation/acceptable_use.html

Department of the Interior (DOI) Memo, *Policies on Limited Personal Use of Government Equipment and Telephone Use*
http://ncc.fws.gov/security/security_v2/docs/Berry_Letter.doc

Department of the Interior (DOI) *Certification and Accreditation Guide*
http://ncc.fws.gov/security/security_v2/docs/CA_Guide_Ver%201.1_(10Jul03).doc

Department of the Interior (DOI) *System Test and Evaluation Guide*
http://ncc.fws.gov/security/security_v2/docs/ST&E_Guide_9-25-03.pdf

Department of the Interior (DOI) *System Security General Support System (GSS) Planning Guide and Template*
http://ncc.fws.gov/security/security_v2/docs/SSP_GSS/General_Support_System_(GSS)_Security_Planning_Guide.doc

Department of the Interior (DOI) *System Security Major Application (MA) Planning Guide and Template*
http://ncc.fws.gov/security/security_v2/docs/SSP_MA/Major_Application_(MA)_Security_Planning_Guide.doc

Department of the Interior (DOI) *Risk Assessment Guide*
http://ncc.fws.gov/security/docs/RA/Risk_Assessment_Guide.doc

Department of the Interior (DOI) *Information Technology (IT) System Contingency Planning Guide*
http://ncc.fws.gov/security/docs/CP/DOI_CP_Guide-final.doc

Department of the Interior (DOI) *Information Technology (IT) Asset Valuation Guideline*
http://ncc.fws.gov/security/security_v2/docs/AV/DOI_IT_Asset_Valuation_Guide_-_Master_corrected.doc

Department of the Interior (DOI) *Privacy Impact Assessment (PIA) and Guide*
http://www.doi.gov/ocio/privacy/DOI%20PIA_03.01.04.doc

Department of the Interior (DOI) *Computer Security Incident Response Handbook*
http://ncc.fws.gov/security/security_v2/docs/DOI_Incident_Handling_Final-V1_070103.doc

Department of the Interior (DOI) *Technical Reference Model*
www.doi.gov/ocio/architecture

Department of the Interior (DOI) *IT Security Awareness Training*
http://www.doi.gov/training/itsecurity/

Department of the Interior (DOI) *System Development Life Cycle (SDLC) Security Integration Guide*
http://ncc.fws.gov/security/security_v2/docs/SDLC_Security_Integration_Guide_for_DOI_IT_Systems.pdf

Department of the Interior (DOI) *Management Control and Audit Follow-up Handbook*
http://www.doi.gov/pfm/mac/2003/mgmt_control_handbook.pdf

U.S. Fish and Wildlife References

U.S. Fish and Wildlife Service (USFWS) Manual Chapter 270 FW 7 - *Automated Information System Security*
http://policy.fws.gov/270fw7.html

- Exhibit 1: *System Security Plans*
  http://policy.fws.gov/e1270fw7.html
- Exhibit 2: *Personal Computer Security*
  http://policy.fws.gov/E2270fw7.html
- Exhibit 3: *Password Controls*
  http://policy.fws.gov/e3270fw7.html

- Exhibit 4: *Physical Security*
  http://policy.fws.gov/e4270fw7.html

U.S. Fish and Wildlife Service (USFWS) Director's Order No. 103 - Subject: *Electronic Mail and Management of Electronic Records*
http://policy.fws.gov/do103.html

U.S. Fish and Wildlife Service (USFWS) *IT Appropriate Use Policy*
http://ncc.fws.gov/security/security_v2/ref_docs/rules.shtml

U.S. Fish and Wildlife Service (USFWS) *Computer Security Incident Response Team (CSIRT) Handbook*
http://ncc.fws.gov/security/security_v2/docs/CSIRT/CSIRT_Handbook_070904.pdf

U.S. Fish and Wildlife Service (USFWS) Information Technology (IT) Bulletin 2003-007 *Interim Information Security Incident Reporting Process*
http://ncc.fws.gov/library/getDoc.cfm?DocID=20020072

U.S. Fish and Wildlife Service (USFWS) Plan of Action and Milestones (POA&M) Guide
http://place.url.here.

U.S. Fish and Wildlife Service (USFWS) *Information Technology Security Cost Estimation Guide*
http://ncc.fws.gov/security/security_v2/docs/FWS_IT_Security_Cost_Estimation_Guide_v9.doc

U.S. Fish and Wildlife Service (USFWS) *System Development Life Cycle Guidebook*
http://ncc.fws.gov/security/security_v2/docs/USFWS_SDLC_Guide_March_2005.pdf

U.S. Fish and Wildlife Service (USFWS) *Security and Suitability Program Handbook*
http://ncc.fws.gov/security/security_v2/docs/USFWS_Security_and_Suitability_Program_Handbook.pdf